Audit des systèmes d'information

ECTS : 3

Description du contenu de l'enseignement :

1. Audit des Systèmes d'Information
2. Audit des Processus Opérationnels
3. Audit de Sécurité

4. Audit protection des données personnelles

1. Audit des Systèmes d'Information - Introduction : acteurs et types d'audit, démarche d'audit et facteurs de succès, notions de risques - Contrôle interne et normes - Typologie de contrôles et General IT controls et leurs domaines - La gestion des changements - Audit/ Revue de projet informatique.
2. Revue des processus opérationnels - Comprendre les processus opérationnels, décrire un cycle opérationnel (7 cycles) et en comprendre l'importance dans la gestion d'une entreprise, comprendre les composants et les flux des transactions, identifier les risques et les activités de contrôle - Comprendre la séparation des fonctions : les principes, les 4 étapes et les outils.
3. Audit de Sécurité : Politique, organisation et administration de la sécurité -
Introduction: *Introduction aux normes ISO 27000 et facteurs clés de succès
*Gestion des risques : comprendre la démarche, la matrice et le traitement et les types de contrôles de sécurité - Politique de sécurité : comprendre son objectif et sa structure - Organisation de la sécurité : comprendre comment gérer la sécurité de l'information au sein de l'organisation, comprendre les différents rôles et leur positionnement notamment le Responsable de la Sécurité des Systèmes d'Information (RSSI) - Classification et contrôle des actifs : comprendre comment maintenir une protection appropriée des actifs de l'organisation, leurs catégories et classification - Sécurité du personnel
- Sécurité physique :
*Sécurité de l'environnement, risques externes et leur prévention
*Risques internes à travers la sécurité des locaux et le contrôle d'accès physique - Gestion des communications et des opérations : objectif et procédures et mesures de protection - Principes de sécurité logique – Contrôle d'accès : authentification, intégrité, confidentialité et gestion des accès aux systèmes et monitoring - Développement et maintenance des systèmes : comprendre les exigences de sécurité des systèmes et la structure d'un projet - Gestion des incidents : les différents cycles - Gestion de la continuité d'activité : comprendre le plan de Business Continuity - Conformité : comprendre la conformité aux exigences légales et l'importance d'audits de sécurité réguliers (et des tests d'intrusion).

4. Données personnelles - Audit de conformité afin de veiller à ce que l'entreprise respecte les différentes règlementation et dispose d'un process conforme

Compétence à acquérir :

1. Audit des Systèmes d'Information - Comprendre les différents acteurs et types d'audit, la démarche et facteurs de succès - Comprendre le contrôle interne et ses normes, les différents types de contrôles ainsi que les General IT controls et leurs domaines - Introduction à la gestion des changements des applications, des bases de données, des systèmes d'exploitation et des réseaux - Audit/Revue de projet informatique : connaitre les types et tailles de projets informatiques, les processus de gestion de projet et de développement.
2. Revue des processus opérationnels - Capacité à comprendre les processus opérationnels, à décrire les 7 cycles opérationnels et en comprendre l'importance dans la gestion d'une entreprise, connaitre les composants et les flux des transactions, possibilité à identifier les risques - Comprendre l'activité de séparation des fonctions, ses principes de bases et ses 4 étapes
3. Audit de Sécurité : Politique, organisation et administration de la sécurité - Connaitre les différentes normes ISO 27000 - Comprendre la démarche de gestion des riques, la matrice et le traitement et connaitre les différents types de contrôles de sécurité - Politique de sécurité : comprendre son objectif et la structure du document - Organisation de la sécurité : comprendre le fonctionnement de la sécurité de l'information au sein de l'organisation, les différents rôles et leur positionnement notamment le RSSI - Classification et contrôle des actifs : comprendre comment il faut maintenir une protection appropriée des actifs de l'organisation, connaitre les différentes catégories et leur classification - Sécurité du personnel : comprendre les objectifs de la

mise en place de la sécurité dans la définition des postes et des ressources - Sécurité physique : connaitre les risques externes et internes et leur prévention, comprendre le contrôle d'accès et les mesures à mettre en place - Gestion des communications et des opérations : comprendre son importance et ses procédures et repsonsabilités ainsi que différents mesures de protection à mettre en place - Principes de sécurité logique – Contrôle d'accès : connaitre les 3 principes de sécurité : authentification, intégrité, confidentialité. Comprendre les règles de gestion de l'accès à l'information dans l'entreprise - Développement et maintenance des systèmes : comprendre les exigences de sécurité des systèmes et les phases d'un projet - Gestion des incidents : connaitre les étapes de gestion des incidents - Gestion de la continuité d'activité : connaitre les 3 étapes clés du BCP - Conformité : comprendre la conformité aux exigences légales et réglementaires ainsi que l'importance d'audits de sécurité réguliers (et des tests d'intrusion).

4. Données personnelles - Connaître le droit à la protection des données personnelles - audit de conformité - gestion des droits - gestion des incidents - transferts - tiers - outils de conformité

Mode de contrôle des connaissances :

Cas pratique + QCM